

## UNITED STATES DISTRICT COURT

for the  
Southern District of Ohio

2019 SEP -5 PM 3:00

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)INFORMATION THAT IS STORED AT PREMISES  
CONTROLLED BY GOOGLE LLC

Case No.

3:19 mj 531

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):  
SEE ATTACHMENT A.

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):  
SEE ATTACHMENT B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

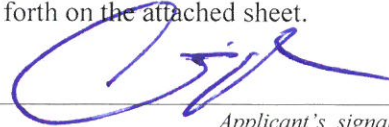
The search is related to a violation of:

Code Section  
18 U.S.C. 922(u)

Offense Description  
Theft of Firearms from a Federal Firearms Licensee

The application is based on these facts:  
See Attached Affidavit.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

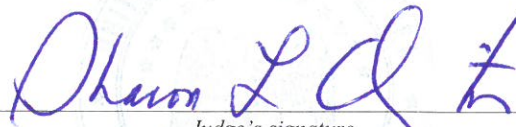
Chris Reed, Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 9-5-19

City and state: Dayton, Ohio



Judge's signature

Sharon L. Ovington, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT  
FOR SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF  
INFORMATION THAT IS STORED AT  
PREMISES CONTROLLED BY GOOGLE  
LLC

**FILED UNDER SEAL**

Case No. 3:19-mj-00531

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, Chris Reed, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a warrant to search information that is stored at premises controlled by Google LLC (Google), a provider of electronic communications service and remote computing service headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a warrant under 18 U.S.C. § 2703(c)(1)(A) to require Google to disclose to the government the information further described in Attachment B I. The government will then review that information and seize the information that is further described in Attachment B II.

2. I have been employed with the U.S. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) as a Special Agent (S/A) since May 2008. Prior to my employment with ATF, I received additional law enforcement training at the Indianapolis Police Department's Police Academy. I was a sworn police officer with the Indianapolis Metropolitan Police Department (IMPD) for approximately (8) years. As a police officer, I conducted investigations in the duty capacity as a uniform officer, narcotics detective and as an ATF Task Force Officer. I have been

involved in numerous investigations of Federal firearms and narcotic violations. These investigations have resulted in the arrest and conviction of criminal defendants. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

3. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C § 922(u) (Theft of Firearms from a Federal Firearm Licensee), have been committed at the location of 1171 West Third Street, Dayton, Ohio. There is also probable cause to search the information described in Attachment A for evidence of these crimes further described in Attachment B.

#### **JURISDICTION**

4. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. Specifically, the Southern Judicial District of Ohio “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

#### **BACKGROUND RELATING TO GOOGLE AND RELEVANT TECHNOLOGY**

5. Based on my training and experience, I know that cellular devices, such as mobile telephone(s), are wireless devices that enable their users to send and receive wire and/or electronic communications using the networks provided by cellular service providers. In order to send or receive communications, cellular devices connect to radio antennas that are part of the cellular network called “cell sites,” which can be mounted on towers, buildings, or other infrastructure. Cell sites provide service to specific geographic areas, although the service area of a given cell site will depend on factors including the distance between towers. As a result, information about what



cell site a cellular device connected to at a specific time can provide the basis for an inference about the general geographic location of the device at that point.

6. Based on my training and experience, I also know that many cellular devices such as mobile telephones have the capability to connect to wireless Internet (“Wi-Fi”) access points if a user enables Wi-Fi connectivity. Wi-Fi access points, such as those created through the use of a router and offered in places such as homes, hotels, airports, and coffee shops, are identified by a service set identifier (“SSID”) that functions as the name of the Wi-Fi network. In general, devices with Wi-Fi capability routinely scan their environment to determine what Wi-Fi access points are within range and will display the names of networks within range under the device’s Wi-Fi settings.

7. Based on my training and experience, I also know that many cellular devices feature Bluetooth functionality. Bluetooth allows for short-range wireless connections between devices, such as between a mobile device and Bluetooth-enabled headphones. Bluetooth uses radio waves to allow the devices to exchange information. When Bluetooth is enabled, a mobile device routinely scans its environment to identify Bluetooth devices, which emit beacons that can be detected by mobile devices within the Bluetooth device’s transmission range, to which it might connect.

8. Based on my training and experience, I also know that many cellular devices, such as mobile telephones, include global positioning system (“GPS”) technology. Using this technology, the phone can determine its precise geographical coordinates. If permitted by the user, this information is often used by apps installed on a device as part of the app’s operation.

9. Based on my training and experience, I know Google is a company that, among other things, offers an operating system (“OS”) for mobile devices, including cellular phones,

known as Android. Nearly every cellular phone using the Android operating system has an associated Google account, and users are prompted to add a Google account when they first turn on a new Android device.

10. In addition, based on my training and experience, I know that Google offers numerous online-based services, including email (Gmail), navigation (Google Maps), search engine (Google ), online file storage (including Google Drive, Google Photos, and YouTube), messaging (Google Hangouts and Google Allo), and video calling (Google Duo). Some services, such as Gmail, online file storage, and messaging, require the user to sign in to the service using their Google account. An individual can obtain a Google account by registering with Google , and the account identifier typically is in the form of a Gmail address. Other services, such as Google Maps and YouTube, can be used while signed in to a Google account, although some aspects of these services can be used even without being signed in to a Google account.

11. In addition, based on my training and experience, I know Google offers an Internet browser known as Chrome that can be used on both computers and mobile devices. A user has the ability to sign in to a Google account while using Chrome, which allows the user's bookmarks, browsing history, and other settings to be synced across the various devices on which they may use the Chrome browsing software, although Chrome can also be used without signing into a Google account. Chrome is not limited to mobile devices running the Android operating system and can also be installed and used on Apple devices.

12. Based on my training and experience, I know that, in the context of mobile devices, Google 's cloud-based services can be accessed either via the device's Internet browser or via apps offered by Google that have been downloaded onto the device. Google apps exist for, and can be downloaded to, phones that do not run the Android operating system, such as Apple devices.

13. Based on my training and experience, I know that Google collects and retains location data from devices running the Android operating system when the user has enabled Google location services. Google then uses this information for various purposes, including to tailor search results based on the user's location, to determine the user's location when Google Maps is used, and to provide location-based advertising. In addition, I know that Google collects and retains data from non-Android devices that run Google apps if the user has enabled location sharing with Google. Google typically associates the collected location information with the Google account associated with the Android device and/or that is signed in via the relevant Google app. The location information collected by Google is derived from sources including GPS data, information about the cell sites within range of the mobile device, and information about Wi-Fi access points and Bluetooth beacons within range of the mobile device.

14. Based on my training and experience, I also know that Google collects and retains information about the user's location if the user has enabled Google to track web and app activity. According to Google, when this setting is enabled, Google saves information including the user's location and Internet Protocol address at the time they engage in certain Internet- and app- based activity and associates this information with the Google account associated with the Android device and/or that is signed in with the relevant Google app.

15. Location data, such as the location data in the possession of Google, can assist in a criminal investigation in various ways. As relevant here, I know based on my training and experience that Google has the ability to determine, based on location data collected via the use of Google products as described above, mobile devices that were in a particular geographic area during a particular time frame and to determine which Google account(s) those devices are associated with. Among other things, this information can inculpate or exculpate a Google account



holder by showing that he was, or was not, near a given location at a time relevant to the criminal investigation.

16. Based on my training and experience, I know that when individuals register with Google for an account, Google asks subscribers to provide certain personal identifying information. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

17. Based on my training and experience, I also know that Google typically retains and can provide certain transactional information about the creation and use of each account on its system. This information can include the date on which the account was created, the length of service, records of login (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, Google often has records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the account.

**PROBABLE CAUSE**

18. On or about August 29, 2019, at approximately 12:32 p.m., three unidentified suspected male individuals conducted an armed robbery of the Ohio Loan Company Inc., located at 1171 West Third Street, Dayton, Ohio. The Ohio Loan Company Inc., is a Federal Firearm Licensee (FFL). This business is equipped with video surveillance equipment, which was functioning at the time and recorded the events.

19. At approximately 12:32 p.m., the three unidentified suspected male individuals entered the Ohio Loan Company armed with handguns. During the course of the robbery, the unidentified suspected male individuals pointed their firearms at business employees and a customer as they moved about inside the store. One of the suspects approached a glass display case that contained multiple handguns and appeared to strike the display case, shattering the glass. A short time later, the same suspect proceeded to another glass display and attempted to break the top section by striking it with his firearm. After an unsuccessful attempt, the suspect then discharged his handgun into the glass display case, this time breaking the glass. The unidentified suspects proceeded to take the firearms from the display cases and appeared to have placed them in bag. Moments later the three unidentified suspected male suspects exited the store and fled on foot.

20. The Ohio Loan Company Inc. later confirmed there were twenty-seven (27) firearms and jewelry unlawfully taken from the premises during the robbery.

21. Based on my training and experience, I know that when people act in concert with one another to commit a crime, they frequently utilize cellular telephones to communicate with each other through voice calls, text messages, and emails. These cellular telephones allow them to plan, coordinate, execute, and flee the scene of crimes. Furthermore, I know people often take



pictures utilizing their cellular telephones that may implicate them in a crime, i.e., possessing a firearm, posing with large quantities stolen items, or large amounts of cash.

22. Also, based on my training, experience, and knowledge, records retained by Google may show whether the unidentified suspects' mobile devices were in or around the relevant locations in Dayton, Ohio, namely 1171 West Third Street, Dayton, Ohio, at or during the time of the robbery which occurred at the date, time, and location described above and, more particularly, identified in Attachment A.

23. The latitude and longitude coordinate for the address of 1171 West Third Street, Dayton, Ohio, is Latitude: 39.7561002, Longitude: -84.2136938.

24. Based on the forgoing, there is probable cause to believe that violations of 18 U.S.C. § 922(u), theft of firearms from a Federal Firearms Licensee, occurred and that Google location data may aid in identifying the three unknown male suspects who armed robbed the FFL. Among other things, this information can inculcate or exculpate a Google account holder by showing that he/she was, or was not, near a given location at a time relevant to the criminal investigation.

25. In order to facilitate the manageable disclosure of and search of this information, the proposed warrant contemplates that Google will disclose the information to the government in stages rather than disclose all of the information for which the government has established probable cause to search at once. Specifically, as described in Attachment B.I:

a. Google will be required to disclose to the government an anonymized list of devices that specifies information, including the corresponding unique device ID, timestamp, coordinates, and data source, if available, of the devices that reported their location within the Target Location described in Attachment A, during the time period described in Attachment A;

b. The government will then review this list in order to prioritize the devices about which it wishes to obtain associated information; and

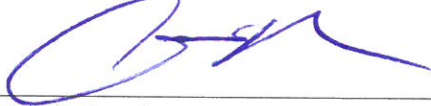
c. Google will then be required to disclose to the government the information identifying the Google account(s) for those devices about which the government further inquires.

**CONCLUSION**

26. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the computer systems in control of Google there exists evidence of a crime, contraband and/or fruits of a crime. I therefore respectfully request that the Court issue the proposed warrant, pursuant to 18 U.S.C. § 2703(c).

27. I further request that the Court direct Google to disclose to the government any information described in Section I of Attachment B that is within its possession, custody, or control. Because the warrant will be served on Google, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Chris Reed  
Special Agent  
Bureau of Alcohol, Tobacco, Firearms and  
Explosives

Subscribed and sworn to before me on September 5, 2019.



HON. SHARON L. OVINGTON  
UNITED STATES MAGISTRATE JUDGE

## ATTACHMENT A

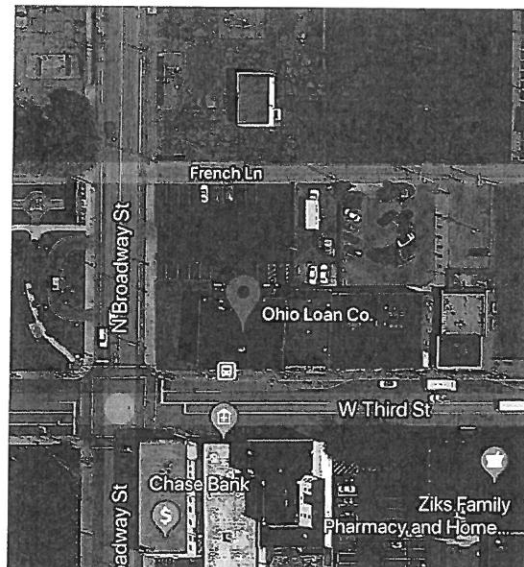
### **Property To Be Searched**

This warrant is directed to Google LLC and applies to:

- (1) location history data, sourced from methods including GPS, Wi-Fi, and Bluetooth, generated from devices and that reported a device location within the geographical region bounded by the latitudinal and longitudinal coordinates, dates, and times below (“Initial Search Parameters”); and
- (2) identifying information for Google Accounts associated with the responsive location history data.

### Initial Search Parameters

- Date: August 29, 2019
- Time Period: 12:00 p.m. to 1:00 p.m. (Eastern Standard Time)
- Target Location: Geographical area identified as a radius of 50 meters around Latitude: 39.7561002, Longitude: -84.2136938





**ATTACHMENT B**

**Particular Items to Be Seized**

**I. Information to be disclosed by Google LLC**

Google LLC shall provide responsive data (as described in Attachment A) to the government pursuant to the following process:

1. Google LLC shall query location history data based on the Initial Search Parameters specified in Attachment A.

2. For each location point recorded within the Initial Search Parameters, Google LLC shall produce to the government anonymized information specifying the corresponding unique device ID, timestamp (in Eastern Standard Time), coordinates, display radius, and data source, if available (the “Anonymized List”).

3. The government shall review the Anonymized List in order to prioritize the devices about which it wishes to obtain identifying information.

4. Google LLC is required to disclose to the government identifying information, as defined in 18 U.S.C. § 2703(c)(2), for the Google Account associated with each device ID about which the government inquires.

**II. Information to Be Seized**

All information described above in Section I that constitutes evidence of violations of 18 U.S.C § 922(u) (Theft of Firearms from a Federal Firearm Licensee), and identifies cellular telephones used in the specified area during the specified time period.